BY THE ORDER OF COMMANDER
AIR MOBILITY COMMAND

AMC INSTRUCTION 33-202, VOLUME 1

1 JANUARY 2002

Communications and Information

INFORMATION ASSURANCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: 805 CSS/SCBSM
(SMSgt Alan McClellan)
Certified by: AMC CG/CC (Col Touhill)
Supersedes AMCI 33-202, Volume 1, 1 July 1999
Pages: 19
Distribution: F

This instruction supplements direction and guidance in DOD, Air Force, Air Force Systems Security Instructions and Air Force Systems Security Memorandum for implementation of Information Assurance (IA) programs at MAJCOMs, Numbered Air Forces (NAF), AMC wings, direct reporting units (DRU) and field operating agencies (FOA).

Conflicts between this document and other documents will be resolved by the AMC IA Programs/Policy Element at 805 CSS/SCBSM; 861 South Drive, Room 156; Scott AFB IL 62225-5101, DSN 576-4049/3727/4070.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed. The 805 CSS/SCBS web site is listed as a source of supplemental guidance. Clarification on the Certification and Accreditation (C&A) and functional review processes is located there.

1. Purpose.

1.1. Establish AMC policy to supplement existing Air Force policy pertaining to management of all IA programs at MAJCOM, NAFs, wings and FOAs/DRUs. Inform customers that supplemental guidance on various IA topics can also be obtained by contacting 805 CSS/SCBSM or accessing the following web site: **https://amccg.scott.af.mil/cgHome/805/securityFlight/index.cfm**

2. Applicability and Scope.

2.1. This publication applies to all.

2.1.1. AMC military, civilian and contractor personnel under contract to develop, acquire, deliver, use, operate or manage an Air Force information system (including embedded).

2.1.2. Air National Guard (ANG) units and other organizations (e.g., Army, Navy, USTRANSCOM, etc.) when using AMC information system assets; and when included as part of an agreement (e.g., memorandum of agreement or service level agreement). Information systems assets refer to computers, applications, local area networks and base metropolitan or wide area networks.

2.1.3. This instruction will not apply to AMC-gained Air Force Reserve Command (AFRC) wings on AFRC bases except for users of AMC C2 systems. All requests for metrics from AFRC units will be addressed to AFRC/SCMD, IA Branch.

2.1.4. This instruction applies to the ANG when published in the ANG Index (ANGIND) 2.

2.1.5. All users of AMC C2 systems, regardless of host command.

3. Changes, Revisions and Deviations. Forward suggested changes, revisions or deviations to 805 CSS/SCBSM. Contact information for 805 CSS/SCBSM is provided prior to "Summary of Revisions" at the beginning of this instruction.

4. Glossary of References and Supporting Information.

4.1. Air Force Manual (AFMAN) 33-270, *Command, Control, Communications and Computer* (*C4) Systems Security Glossary*.

4.2. A consolidated list of C&A references can be found in **Attachment 1**.

4.3. AMC network security policies are discussed in-depth in AMCI 33-202 Volume 2 (awaiting publication).

5. Contractor and Foreign National Access (FNA) to Government Networks. DOD 5200.2-R and AFI 33-202 require contractors to have a "National Agency Check" and receive written approval from the system Designated Approving Authority (DAA) and the DAA of all systems exchanging information before receiving access. HQ AMC/SC is the DAA for all AMC C2 systems.

5.1. U.S. Contractors. See **Attachment 2** for instructions for obtaining DAA approval for U.S. contractors to access AMC information systems.

5.2. Foreign Nationals. Until formalized FNA procedures are resolved within AMC, program managers or system administrators will notify the DAA by memorandum semiannually of the number and origin of foreign nationals accessing Air Force systems. See **Attachment 3** for the required memorandum format. Whenever National Agency Checks (NAC) are possible for foreign nationals, the full FNA requirements from AFI 33-202 and AFSSI-5027 still apply.

6. Computer/Information Systems C&A.

6.1. C&A General Requirements. All government computer/information systems that contain a processor and non-volatile memory must be accredited by the DAA before being placed into operation. Accreditation requirements also apply to computers and information systems to be installed or used within aircraft when those systems connect to AMC networks.

6.1.1. Computer/information systems include workstations, laptop computers, personal digital assistants, printers, digital photocopiers, servers, firewalls, dial-up servers and any new or existing technology that contains a processor and non-volatile memory.

6.1.1.1. When classified systems are accredited, apply the appropriate checklist that includes Emission Security (EMSEC) requirements. See paragraph **9.** and AFI 33-214, *Emission Security Countermeasure* Reviews for additional EMSEC guidance.

6.1.2. For purposes of efficiency, and to comply with the Paperwork Reduction Act, batch C&A of similar systems are not only authorized but highly encouraged. During C&A, multiple systems to be accredited can be listed on the appropriate AMC Form 1014, **Certification & Accreditation Statement**, (e.g., a workcenter would generate one approval C&A package for 50 Windows 2000 CPUs (model xxx) for NIPRNET connectivity.)

6.1.3. New server and network infrastructure equipment connected to the NIPRNET or SIPRNET will not be activated without a completed AMC Form 1014, Certification and Accreditation package, and Certificate to Operate (CTO) approved through HQ AMC/SCYB or at least an Interim Approval to Operate (IATO) pending completion of C&A and CTO requirements.

6.1.3.1. Copies of completed AMC Forms 1014 reflecting DAA approval and signed CTO or signed IATO must be attached to all AF Form 3215 requests to connect new network devices.

6.1.3.1.1. No Network Control Center will connect devices without a completed approval package (in the case of MS-Windows ™ workstations) or a CTO/ICTO signed by the AMC CIO.

6.1.3.2. Submit C&A packages for network infrastructure equipment and servers to 805 CSS/SCBSM for coordination with the appropriate DAA. The accreditation documentation must be submitted in DOD Information Technology Security Certification Accreditation Process (DITSCAP), format (see 805 CSS/SCBS web page for DITSCAP requirements) with a completed AMC Form 1014.

6.1.3.3. See **Attachment 4** which identifies minimum requirements for accrediting network backbone equipment (hubs, routers, switches) and servers.

6.1.3.4. See **Attachment 5** which provides instructions for submitting completed AMC Form 1014 and C&A packages with LOW residual risks to HQ AMC for CTO and DAA signature.

6.1.4. All MS-Windows ™ based networked workstations must be approved using the AMC Form 1014-1 (**Security Certification & Accreditation Statement** for MS Windows workstations, stand-alone computers and Personal Digital Assistants (PDAs), and MAJCOM provided security checklist confirming all Time Compliance Network Orders (TCNO) are applied and all medium and high risks have been eliminated by conducting an Internet Security Scanner (ISS) scan. Locally developed security checklists may be utilized in the absence of a MAJCOM or Network Operations and Security Center (NOSC) provided security checklist, after approval by the AMC C&A review team.

6.1.4.1. AFI 33-202, paragraph 3.9. prohibits use of modems in any workstation or laptop computer connected to the base network. To meet this requirement, do not purchase new computer systems with modems installed. However, laptop computers may require modems to meet mission requirements. In such cases, laptop computers with modems must not be simultaneously connected to networked docking stations and phone lines.

6.1.4.2. All MS-Windows ™ based standalone computers must be approved using the AMC Form 1014-1 and security checklist.

6.1.4.3. See **Attachment 6** which identifies minimum requirements for approved networked MS Windows ™ workstations that don't utilize modems, file sharing or print sharing. This documentation will be maintained at each base but will not be forwarded to HQ AMC.

6.1.4.4. See **Attachment 6** which identifies minimum requirements for approving standalone computers. This documentation will be maintained at each base but will not be forwarded to HQ AMC.

6.1.5. See the 805 CSS/SCBS web page for more information on C&A requirements.

6.2. DAA Assignment.

6.2.1. C&A DAA Roles and Responsibilities**.** DAA functions for ALL AMC servers and network infrastructure equipment are performed at HQ AMC in conformance with AMC/CC letter dated 20 Mar 02, Subject: Assignment of AMC DAA.

6.2.1.1. HQ AMC/SC is the DAA for SIPRNET and NIPRNET systems and networks. This includes all servers (email, file, web, File Transfer Protocol, etc.) and equipment that constitutes the backbone of base networks (intelligent hubs, routers and switches). However, this does not include servers and networks processing Top Secret or Secret sensitive compartmented information.

6.2.1.2. Approving Authority for Standard Office Administrative Workstations**.** Approval authority for networked administrative MS Windows ™ based workstations (without file or print sharing enabled, without a modem, and not used as a web server) is delegated to the flight commander, element chief, division or branch chief.

6.2.1.2.1. Approval authority for standalone MS Windows ™ computers is delegated to the flight commander, element chief, division or branch chief.

6.2.1.3. Contact 805 CSS/SCBSM for questions regarding assignment of DAA (or Approval Authority) for specific systems to be accredited whenever adequate guidance is not provided by this instruction.

6.3. General C&A Guidance.

6.3.1. Use AMC Form 1014, System C&A Statement, to document coordination, review and DAA approval of all C&A packages for systems requiring formal accreditation at HQ AMC (servers, network infrastructure equipment, non-MS Windows ™ workstations and network infrastructure equipment). All DITSCAP documents must be submitted with AMC Form 1014 requests.

6.3.2. Use AMC Form 1014-1 and AMC approved workstation minimal security activity checklist (see **Attachment 6**) to document approval of MS Windows ™ workstations that don't utilize modems, file sharing, or print sharing. AMC Form 1014-1 is filed at each organization after local approval.

6.3.2.1. Use AMC Form 1014-1, Security Certification Accreditation Consolidation Statement, and AMC approved standalone security checklist to document accreditation of standalone computers.

6.3.3. Use AMC Form 1014-2 to consolidate quarterly AMC Form 1014 requests for DAA signature at HQ AMC. Ensure all Tracking Control Numbers from AMC Forms 1014 being submitted for DAA approval are listed on the AMC Form 1014-2 with any blank Tracking Control Number slots on the AMC Form 1014-2 being filled with "N/A". After AMC Form 1014-2 is signed, a photocopy will be attached to each subordinate AMC Form 1014 that is listed on the AMC Form 1014-2.

6.3.4. The 805 CSS/SCBS web site provides instructions for preparing and processing AMC Forms 1014, 1014-1 and 1014-2.

6.3.5. Failure to comply with TCNOs will void C&A packages unless the DAA has accepted additional risk in writing.

6.3.6. ***CAUTION:*** Remember that when documenting vulnerabilities of classified systems during C&A activities, such documentation must be classified to the maximum classification of information contained on those systems.

6.3.6.1. If submitting classified information as part of C&A packages, ensure DOD approved methods of transmitting classified material are utilized.

6.4. Operation of LOW Risk Systems awaiting DAA signature on AMC Form 1014 for completed C&A packages.

6.4.1. Networked systems (other than MS Windows-based workstations documented on AMC Form 1014-1) having no residual risks above LOW as identified after a complete certification effort may be considered accredited and placed into operation while awaiting formal DAA signature if the following conditions are met:

6.4.1.1. Comprehensive security test and evaluation has been conducted and all remaining residual risks are LOW (where possible, LOW risks will be corrected unless impractical).

6.4.1.2. The Certifier has signed the AMC Form 1014 attesting to the conduct of the security testing and the results are accurate.

6.4.1.3. 805 CSS/SCBSM (MAJCOM Information Assurance Policy Element) has reviewed the SSAA for completeness and has concurred on the AMC Form 1014.

6.4.1.4. An Information Systems Security Officer (ISSO), is appointed in writing to ensure no additional configuration changes are made to the system and no additional software is loaded on the system except TCNO.

6.4.1.5. The MAJCOM CIO approves the connection to the AMC enterprise by signing the applicable box on the AMC Form 1014.

6.4.1.5.1. Maintain current ISSO appointment letters on file with the SSAA.

6.4.1.5.2. NOTE: Failure to comply with any TCNO will void CIO approval to operate system.

6.4.1.5.3. ISSO will ensure antivirus signature files are kept current.

6.5. Certificate to Operate (CTO) Procedures. All systems (servers and network infrastructure equipment such as routers, switches, etc.) connecting to the AMC Enterprise will have a CTO signed by the AMC CIO. Legacy systems are exempt from this requirement until they undergo a major upgrade.

6.5.1. Each base will ensure that an AMC CIO approved CTO package is received PRIOR TO connecting new servers and network infrastructure equipment.

6.5.1.1. LOW risk systems approved by the AMC CIO (HQ AMC/SC) for connection prior to DAA approval will receive the required CTO when the AMC Form 1014 is signed by the CIO.

6.5.1.2. Systems with MEDIUM or HIGH residual risk will receive a CTO when residual risks are mitigated to an acceptable level following a detailed administrative review of risks by 805 CSS/SCBSN, CTO processing by HQ AMC/SCYB, and CTO signature by the AMC CIO. This process can take 60-90 days.

6.5.1.3. Contact 805 CSS/SCBSN for any questions regarding this issue.

6.5.2. Prior to connecting/using new workstations or standalone computers utilizing MS-Windows™ operating systems, each base will ensure that the required security checklist and an accompanying AMC Form 1014-1 is on file.

6.5.3. Future guidance on Certificate of Networthiness, CTO and C&A for new systems will be posted on the 805 CSS/SCBS web page.

6.6. Interim Approval to Operate. IATO may be granted in rare cases where accreditation cannot be completed before systems are required to be operational. Before IATO will be considered, the following items must be provided to HQ AMC/SCYB for consideration along with the AMC Form 1014 request: (See **Attachment 7** for memorandum requirements)

6.6.1. Provide a system description (operating system and hardware used, functions performed by system, interfaces to base network or remote devices).

6.6.2. Provide a topology map showing system logical network connections and remote device interfaces.

6.6.3. Describe what physical security requirements exist and how these are currently being met.

6.6.4. Describe communications security (COMSEC) requirements (if any) and how these requirements are currently being met (Reference AFI 33-211 and 33-212).

6.6.5. Describe personnel security requirements and how these requirements are currently being met.

6.6.6. Describe how system privileges are controlled.

6.6.7. Describe system-unique computer security requirements.

6.6.8. Describe network services utilized (File Transfer Protocol, Simple Network Management Protocol (SNMP), etc.).

6.6.9. Apply all TCNO and security patches, and provide a record of what has been applied.

6.6.10. Provide initial ISS scan.

6.6.11. Correct ALL medium or high-level risks or list planned corrective measures to include estimated completion date.

6.6.12. Provide clean ISS scan without medium or high-level risks.

6.7. AMC System Accreditation (C&A) Status Reporting:

6.7.1. Annual collection and reporting of information systems C&A metrics is required by AFPD 33-2 to determine degree of base compliance with Air Force policy.

6.7.2. Each wing IA office is the focal point for monitoring, tracking and reporting the accreditation status of host base systems to 805 CSS/SCBSM. Host units at each base will submit C&A packages to 805 CSS/SCBSM through their wing IA office. Tenant organizations (MAJCOM agencies, etc.) will also provide their own focal points for monitoring, tracking and reporting C&A issues and coordinating all C&A actions with 805 CSS/SCBSM.

6.7.2.1. Each wing IA office or focal point in tenant organizations must appoint personnel to complete required data entry and modification in the AMC C&A database. Each wing IA office and focal point in tenant organizations must send or fax appointment letters for personnel who require capability to enter, edit or retrieve C&A database records to 805 CSS/SCBSM before access will be granted.

6.7.3. Before submitting C&A documentation (for servers and network equipment) to the AMC C&A Review Office (805 CSS/SCBSM), each wing IA office or focal point in tenant organizations will ensure that all required information from AMC Forms 1014, 1014-1 and 1014-2 is entered into the online database (see 805 CSS/SCBS web page for database link). After the C&A documentation is received, reviewed and the applicable DAA accredits by signature, the AMC C&A Review Office (805 CSS/SCBSM) will place the accreditation date in the database which will lock all critical information in the database and prevent modification. If any critical areas are changed on a system, the system will need to be re-accredited.

6.7.4. Although workstations will be approved locally, information must also be entered into the AMC C&A tracking database. Contact 805 CSS/SCBSM to obtain the URL of the online C&A tracking database if you are unable to find it.

6.7.5. Wing IA offices will submit annual C&A metrics for legacy systems in January of each year unless the information has already been entered into the AMC C&A tracking database. Legacy system accreditations expire not later than August 2003.

6.7.6. 805 CSS/SCBSM monitors and reports the accreditation status for HQ AMC assets and will provide annual guidance in an official message when downward directed taskings are received.

7. Information Assurance Assessment and Assistance Program (IAAAP).

7.1. The AMC IAAAP is implemented according to AFI 33-230.

7.2. Biennial and as-required IAAAs are conducted using AMC-expanded checklists based on AF Form 4160**, Information Assurance Assessment and Assistance Program (IAAAP)** Criteria.

7.2.1. The information provided on the standard AF Form 4160 is too vague to properly assess IA programs within AMC. For this reason, AMC has divided the AF Form 4160 questions into subtopics that are required to properly evaluate the various IA disciplines.

7.2.2. The AMC modified AF Form 4160 questions can be located at:
https://amccg.scott.af.mil/cgHome/805/securityFlight/SMSI/4160s.html.

7.2.3. Direct questions or suggestions regarding the AF Form 4160 or subtopics to 805 CSS/SCBSM.

7.3. IAAAs of ANG units will consist of only the COMSEC checklist items, unless otherwise requested by the hosting organization, and approved by AMC CG/CC.

7.4. Reviewed activities must address all findings identified in IAAA reports within 14 days of receipt. Replies must address the specific actions taken to correct and eliminate the basic cause of the findings, provide enough detail to permit effective evaluation and provide an estimated completion date for all open items.

7.5. IAAA findings must remain open until corrected. Open items require 90-day follow-up reporting through command channels to 805 CSS/SCBSM.

7.6. Each reviewing authority must provide a concurrence or nonconcurrence with the corrective actions taken and endorse the report to the next reviewing authority.

7.7. AMC CG/CC is the final authority on determining the adequacy of unit responses to IAAA reports and the closing of individual findings or reports.

7.8. See 805 CSS/SCBS web pages for IAAAP Rating Criteria.

8. Transmitting For Official Use Only (FOUO) Information by E-mail. FOUO information can be transmitted to other agencies within DOD after encryption. Within the Air Force, the encryption requirement is met automatically by the existing Air Force Virtual Private Network (AF VPN) infrastructure. When sending FOUO information to DOD activities outside of the Air Force, separate encryption measures are required unless the receiving DOD component has a VPN directly connected to AF VPN. These separate encryption measures are required to protect FOUO information from possible monitoring by unauthorized personnel when transmitted over public telecommunications systems.

8.1. Manual encryption of FOUO information. To securely transfer FOUO information to recipients outside of the AF VPN, those who transmit such information must utilize a file compression utility that encrypts and provides password protection for archives (such as pkzip.exe or pkunzip.exe). Such programs may be used to prepare unclassified FOUO files for e-mail transfer. Information senders must send encrypted compressed files attached to e-mail messages, along with notification to recipient(s) that passwords for the compressed files will be sent in separate e-mails. Information senders must ensure recipients have the necessary programs to decompress and decrypt any files transferred.

9. AMC Emission Security (EMSEC) Requirements.

9.1. EMSEC Countermeasures Reviews. AFMAN 33-214 Volume 2 mandates Air Force organizations and contractors that require classified computer systems for conducting operations to obtain EMSEC countermeasure reviews by contacting the host wing IA office.

9.2. Before certifying EMSEC countermeasure reviews, wing EMSEC managers must obtain a diagrammed floor plan from the unit OPR showing location of classified systems, unclassified systems, telephones and radios. This is necessary to verify whether system configurations have been modified without obtaining proper documentation. The diagrammed floor plans will be attached to the AFCOMSEC Form 7001 or AF Form 4170, **Emission Security Countermeasures Review**, that are maintained by the base EMSEC manager.

9.3. Computer systems approved by the wing EMSEC manager will not be moved. Movement of these systems invalidates the EMSEC approval and requires another EMSEC evaluation and approval.

JOHN R. BAKER, Lt Gen, USAF
Vice Commander

Attachment 1

CERTIFICATION & ACCREDITATION (C&A) REFERENCES

A1.1. DOD Directive 5200.28 (Security Requirements for Automated Information Systems), DOD Instruction 5200.40 (DOD Information Technology Security Certification and Accreditation Process (DITSCAP)) and AFPD 33-2 (Information Protection) require accreditation before operational use.

A1.2. DOD 8510.1-M (Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual).

A1.3. AFSSI 5027 (Network Security Policy).

A1.4. AFI 33-115 Volume 1 (Network Management).

A1.4.1. **Attachment 3** provides sample service level agreements.

A1.4.2. **Attachment 4** provides task breakdown for system and network support responsibilities

A1.4.3. **Attachment 5** provides network security management checklist

A1.5. AMC Instruction 33-202 Volume 2 (pending publication) will provide supplemental network security policy and additional C&A guidance.

Attachment 2

U.S. CONTRACTOR ACCESS TO AMC INFORMATION SYSTEMS

A2.1. AFSSI-5027, paragraph 5.3.1. and AFI 33-112, paragraph 15 identify requirements for NAC and DAA approval before contractors access government information systems and networks. These requirements also apply to contractor-owned information systems processing government information.

A2.2. To meet these requirements, the approval authority for contractors that are U.S. citizens is hereby delegated to the commander of each unit with contractors who access government information systems.

A2.3. Before approval is given for any contractor that is a U.S. citizen, the unit security manager will submit a memorandum to the appropriate commander that confirms a favorable NAC appears in the Sentinel Key database for each contractor listed on the memorandum. The commander will approve memorandum requests by signature.

A2.4. The approved contractor requests will be kept on file with the unit security manager using AFMAN 37-139, Table 31-4, Rule 15 and courtesy copies will be forwarded to the Base Computer Security Manager within the Communications Squadron.

A2.5. To bring units into compliance that have not previously obtained written approval for U.S. citizen contractors, authorization must be obtained from the appropriate commander within 180 days of this document publication date or access to government information systems and networks must be revoked until the required approval is obtained.

Attachment 3

MEMORANDUM NOTIFYING DAA OF FOREIGN NATIONALS ACCESSING SYSTEMS

DATE

MEMORANDUM FOR (DAA OFFICE SYMBOL)

FROM: (ORIGINATING AGENCY)

SUBJECT: Foreign National Access (FNA) Notification

1. This memorandum officially notifies the DAA of foreign nationals currently accessing (SYSTEM NAME).

COUNTRY OF ORIGIN	NUMBER OF FOREIGN NATIONALS
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

2. Our point of contact for FNA issues is _____ at DSN _____.

SIGNATURE BLOCK OF SYSTEM ADMINISTRATOR OR SECURITY OFFICER

Attachment 4

MINIMUM REQUIREMENTS FOR ACCREDITING NETWORK EQUIPMENT AND SERVERS

A4.1. The equipment governed by this attachment includes all network equipment (smart hubs, routers, switches, etc.) and servers (file servers, web servers, mail servers, firewalls, etc.).

A4.1.1. Accredit like-equipment together in single packages (C&A servers, switches, etc.).

A4.2. Complete all steps below before submitting certification and accreditation packages for servers:

A4.2.1. Appoint a network security officer in writing to ensure configurations are continually updated to maintain security. Update appointment letters annually.

A4.2.2. Use AMC Form 1014 to identify equipment being accredited and to summarize C&A efforts.

A4.2.3. The System Security Authorization must be completed according to DITSCAP requirements and all DITSCAP appendices must be present. (See 805 CSS/SCBS web page.)

A4.2.4. Ensure all checklists included with SSAA or DITSCAP appendices include the date and identify who completed the required actions.

A4.2.4.1. Written explanation must be provided for any checklist items that are marked as "N/A" explaining why items were not applicable.

A4.2.5. ISS scan must be run by your local NCC, certified ISS personnel (with administrator privileges) or by the AMC NOSC for submission with C&A packages.

A4.2.5.1. Provide an ISS output report or other printed documentation with date showing ISS scans for workstations to be accredited have no remaining HIGH or MEDIUM vulnerabilities.

A4.2.5.2. Any false HIGH or MEDIUM vulnerabilities on ISS scans are acceptable only when documentation is included in C&A package showing how the remaining vulnerabilities were proven to be false positive readings. All LOW vulnerabilities must be corrected that conflict with AF policy (i.e. – passwords not set to expire).

A4.2.5.3. Systems with remaining MEDIUM or HIGH vulnerabilities may be considered for IATO (see **Attachment 7**) if planned corrective measures and estimated completion dates are listed along with vulnerabilities in the system Risk Assessment.

A4.2.5.4. Scans must be current within 30 days when submitted to the AMC IA office (805 CSS/SCBSM) or local Wing IA office.

A4.2.6. Identify all security configuration requirements (in writing) in the Trusted Facility Manual (TFM).

A4.2.6.1. Minimum security configuration requirements for hubs, servers and routers will include control of administrator privileges to a minimum number of personnel, changing default passwords and SNMP public strings and establishing procedures to periodically back up key files such as routing tables, etc.

A4.2.6.2. If a TFM for your operating system/network hardware is not available, contact the AMC IA Office (805 CSS/SCBSM) at DSN 576-4049.

A4.2.6.3. Configure servers/network equipment according to TFM.

A4.2.7. Submit copies of all system configuration, security and contingency-related checklists and operating instructions with the C&A package. These checklists and operating instructions must be reviewed annually for accuracy and updated as required. (These checklists can replace the TFM provided thorough guidance is included to securely configure each applicable server in the event of catastrophic failure.)

A4.2.8. Load all current patches and TCNOs.

A4.2.9. Identify tests that attempt to bypass secure configuration of devices to be accredited. Document planned tests, execute as Security Test & Evaluation (ST&E) and document results of tests as ST&E reports.

A4.2.10. Complete Risk Analysis Report to include all unresolved risks from ISS scan report, any failed and/or incomplete testing from ST&E report, any non-secure external connections and all negative replies on Minimal Security Activity Checklist.

A4.2.11. Summarize all DITSCAP appendices on AMC Form 1014 for all servers/network equipment and submit to 805 CSS/SCBSM in accordance with **Attachment 5** & **Attachment 6**

A4.2.12. Provide documentation of EMSEC Countermeasures Review for all classified servers being accredited. An unclassified memorandum from the base IA office stating an AFCOMSEC Form 7001 has been accomplished and EMSEC requirements have been met is ample documentation. Do not submit classified material, such as completed AFCOMSEC Forms 7001, with the C&A documents.

A4.2.13. Include a Service Level Agreement (SLA) in the C&A package with each unit that controls servers or network backbone equipment connected to the equipment being accredited. For an SLA example, reference AFI 33-115 **Attachment 3**. Be sure that each SLA identifies and accepts all NCC-mandated configuration settings. SLA must also address security issues (such as false positive ISS scan) whenever ISS scans identify any risks other than LOW.

A4.3. Network security policy requirements will be met by AMCI 33-202 Volume 2.

A4.3.1. AMCI 33-202 Volume 2 network security policy may be supplemented as needed.

A4.3.2. All network system administrators (SA) and Workgroup Managers (WMs) must hold copies (electronic or paper) and be familiar with AMCI 33-202 Volume 2.

A4.4. Submit C&A packages to 805 CSS/SCBSM for review and coordination following instructions on the 805 CSS/SCBS web page.

A4.5. After accreditation requirements are completed, 805 CSS/SCBSM will enter accreditation dates in the AMC Accreditation Database and return signed documentation to originating wing IA offices or focal point in tenant organizations.

A4.6. C&A packages and signed AMC Form 1014 must be added to a file plan using AFMAN 37-139 Table 33-25, Rule 5.

A4.6.1. Each Network Security Officer and SA must be familiar with C&A packages and have access to conduct documented annual review of required sections.

Attachment 5

PROCEDURES FOR SUBMITTING LOW-RISK NETWORK EQUIPMENT AND SERVER C&A PACKAGES TO HQ AMC

A5.1. Submit electronic copies of all documents to 805 CSS/SCBSM for initial review (e-mail account: **mailto:805 CSS/SCBSM@scott.af.mil**)

A5.2. 805 CSS/SCBSM will review electronic documents and return documents by e-mail with notes for correction.

A5.3. Correct all deficiencies or errors identified by 805 CSS/SCBSM and return for approval, repeating as necessary until all problems with C&A are resolved.

A5.4. Submit electronic copies of all C&A documents and a hard copy of the AMC Form 1014 signed by the Certifier to 805 CSS/SCBSM.

A5.5. 805 CSS/SCBSM will review entire package and provide recommendations to the AMC CIO (HQ AMC/SC), which the CIO will consider before approving or granting CTO and connection to the network.

A5.5.1. The AMC CIO will normally not provide temporary accreditation or final CTO to any system with MEDIUM or HIGH residual risks.

A5.6. After the AMC CIO signs the AMC Form 1014, 805 CSS/SCBSM will enter accreditation dates in the AMC C&A database and return the signed documentation to the originating wing IA office or the focal point in tenant organizations.

A5.7. At least quarterly, units with approved AMC Forms 1014 from the AMC CIO will consolidate those AMC Forms 1014 onto an AMC Form 1014-2 for formal approval by the appropriate DAA.

A5.7.1. All systems being accredited using a single AMC Form 1014-2 must all belong to the same DAA (Reference paragraph **6.2.** to determine DAA).

A5.7.2. Each AMC Form 1014-2 to be submitted for DAA signature must be submitted to 805 CSS/SCBSM with attached copies of all AMC Forms 1014 that are cited on the AMC Form 1014-2.

A5.7.3. 805 CSS/SCBSM will return AMC Forms 1014-2 to the originating organization for staffing to the appropriate DAA.

A5.8. Signed AMC Forms 1014-2 will then be sent to 805 CSS/SCBSM who will update the AMC accreditation database with the date of DAA approval, and the signed documentation will be returned to the originating wing IA office or the focal point in tenant organizations.

A5.8.1. The originating unit will attach copies of the signed AMC Form 1014-2 to each referenced AMC Form 1014 and maintain accreditation documents in unit file plan according to AFMAN 37-139, Table 33-25, Rule 5.

Attachment 6

PROCEDURES FOR CERTIFYING AND ACCREDITING MS WINDOWS ™ BASED WORKSTATIONS AND STANDALONE COMPUTERS

A6.1. The ISSO or WM and alternate must be appointed in writing and kept on file to ensure configurations are continually updated to maintain accreditation.

A6.1.1. ISSO or WM appointment letters must be updated annually to retain accreditation.

A6.2. Use AMC Form 1014-1 to list workstation(s) or standalone computers to be accredited by CPU serial number and location.

A6.2.1. The WM or ISSO will sign AMC Form 1014-1 as the Certifier.

A6.2.2. The element chief or flight commander signs the AMC Form 1014 as 'Approval Authority' for administrative MS Windows ™ workstations and standalone computers.

A6.3. Complete the appropriate checklist (workstation or standalone) and include the date and signature of the person who performed checklist actions for all systems listed on the AMC Form 1014.

A6.3.1. See 805 CSS/SCBS web page for workstation or standalone security checklist.

A6.3.2. (Workstations only) Load all current patches and TCNOs.

A6.3.3. (Standalone computers only) Label machine “standalone” to reduce likelihood of inadvertent network connection.

A6.3.4. Checklist items marked as “N/A” require statements explaining why items were not applicable.

A6.3.5. An ISS scan must be run by your local NCC, certified ISS personnel (with administrator privileges) or by the AMC NOSC for submission with C&A packages.

A6.3.5.1. ISS reports must show that ISS scans for workstations to be accredited have no remaining HIGH or MEDIUM vulnerabilities.

A6.3.5.2. Any false HIGH or MEDIUM vulnerabilities on ISS scans are acceptable only when documentation is included in C&A package showing how those vulnerabilities were proven to be false positive readings. All LOW vulnerabilities must be corrected that conflict with AF policy (i.e. – passwords not set to expire).

A6.3.5.3. Scans must be current within 30 days when the approving authority approves AMC Form 1014-1.

A6.4. Scans results and security checklist must be attached to each completed AMC Form 1014-1.

A6.5. Classified administrative workstations must also include documentation of EMSEC Countermeasures Review. Contact wing IA offices to request the required EMSEC reviews.

A6.5.1. Documentation of C&A should not include the completed AFCOMSEC Form 7001, AF Form 4170 or any other classified information

A6.5.2. Obtain an unclassified memorandum from the EMSEC manager to include with C&A documentation that certifies EMSEC requirements have been met.

A6.6. Bases will file completed AMC Forms 1014-1 (with ISS scan results and supporting documentation) in file plan using AFMAN 37-139, Table 33-25, Rule 5.

A6.6.1. The originating wing IA office or focal point in tenant organizations will update the AMC accreditation database with the system information and date of approval.

Attachment 7

MEMORANDUM REQUESTING TEMPORARY ACCREDITATION AND INTERIM APPROVAL TO OPERATE (IATO) PENDING COMPLETION OF FULL C&A REQUIREMENTS

MEMORANDUM FOR 805 CSS/SCBSM

FROM: _____

SUBJECT: Interim Approval to Operate (IATO)

1. System Description: (Provide a system description, operating system and hardware used, functions performed by system or similar systems, and interfaces to base network or remote devices).

2. Physical Security: (Describe what physical security requirements exist and how these are currently being met.)

3. Personnel Security Requirements: (Describe personnel security requirements (NAC or security clearance) and how these requirements are verified.)

4. Classified System Requirements: (Describe communications security (COMSEC) requirements for classified servers and how these requirements are currently being met.)

5. System Privileges: (Describe how system privileges are controlled.)

6. System unique computer security requirements: (Describe system-unique computer security requirements.)

7. Network services utilized: (File Transfer Protocol, Simple Network Management Protocol (SNMP), etc.).

8. Time Compliance Network Orders: (Apply all TCNOs and security patches, and provide a record of what has been applied).

9. AMC Form 1014. (Attachment 1). Provide AMC Form 1014 as attachment 1 to identify equipment serial numbers, IP addresses and locations (bldg. & room number) for servers or network infrastructure equipment submitted for IATO.

10. Topology Map. (Attachment 2). Provide a topology map as attachment 2 showing system logical network connections and remote device interfaces.

11. ISS Scan. (Attachment 3). Submit ISS scan results as attachment 3 showing all MEDIUM and HIGH residual risks, as well as all LOW risks that conflict with AF policy, have been corrected. This ISS scan must be run by an individual with administrator privileges, using the most stringent settings, and be less than 30 days old.

12. Residual MEDIUM and HIGH Risks (if any): (List planned corrective measures for unresolved MEDIUM or HIGH level risks and include estimated completion date for correcting those unresolved risks.)

13. Our point of contact for this IATO is _____ at DSN _____.

SIGNATURE BLOCK OF CERTIFIER

Attachments:

1. AMC Form 1014
2. Topology Map
3. ISS Scan Results